iCloud Private Relay Overview

Learn how Private Relay protects users' privacy on the internet.

December 2021

Contents

Introduction

iCloud Private Relay is a new internet privacy service from Apple that allows users with iOS 15, iPadOS 15, or macOS Monterey on their devices and an iCloud+ subscription to connect to the internet and browse with Safari in a more secure and private way.

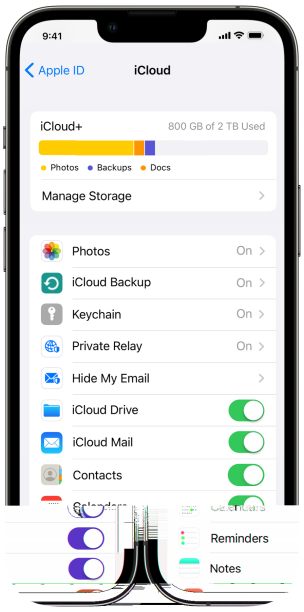
Normally when a user browses the web, basic information related to their web traffic, such as their IP address and DNS records, can be seen by network providers and the websites they visit. This information can be used to determine the user's identity and build a profile of their location and browsing history over time. A user can then be targeted with unwanted ads and marketing campaigns, or have their data combined with additional data and sold to other companies.

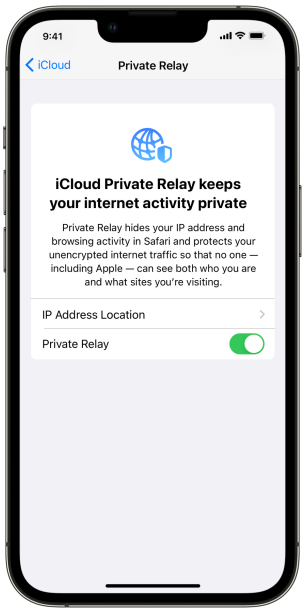
Private Relay helps protect users from this kind of unwanted tracking by ensuring the traffic leaving their devices is encrypted, and by sending their requests through two separate internet relays so that no single entity can combine IP address, location, and browsing activity into detailed profile information. It's built directly into the networking framework of iOS, iPadOS, and macOS, and protects traffic most susceptible to tracking: web browsing and any connections that are unencrypted. As a result, Private Relay protects all web browsing in Safari and unencrypted activity in apps, adding both privacy and security benefits. Private Relay is included with any iCloud+ subscription. This gives Apple device owners an easy way to meaningfully improve their privacy when browsing the internet.

Using Private Relay

Private Relay is simple to use. iCloud+ subscribers can turn on the service from iCloud settings on any Apple device with iOS 15, iPadOS 15, or macOS Monterey or later.

- On an iPhone, iPad, or iPod touch, go to Settings > [your name] > iCloud > Private Relay.





- On a Mac, go to System Preferences > Apple ID > iCloud > Private Relay.

Once it is enabled, users can choose how they'd like Private Relay to convey their location.

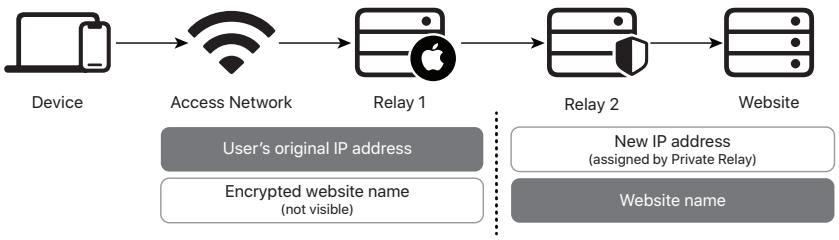
- "Maintain general location" means that Private Relay will choose Relay IP addresses that map to a roughly city-level area consistent with where the user is actually connecting from. This allows sites to use the Relay IP address to show accurate localized content.
- "Use country and time zone" means that Private Relay will choose Relay IP addresses across a broader, more regional area to give added privacy. All Relay IP addresses will still map to the user's original country and time zone.

Private Relay is built using the latest internet standards to maintain a high-performance browsing experience. It is designed so that users can open Safari at any time and browse the web as they always do, while benefiting from the additional privacy and security that the service provides.

Designed for Privacy

Private Relay is built on the principle that IP addresses that identify users need to be separated from the names of websites that users access. To achieve this separation, Apple has engineered an innovative dual-hop architecture in which users' requests are sent through two separate internet relays operated by different entities. Private Relay's dual-hop architecture protects the privacy of users by separating who can observe their IP addresses from who can see the websites they visit.

Private Relay Dual-hop Architecture



When Private Relay is in use, the user's device opens up a connection to the first internet relay (also known as the "ingress proxy"). The software for the first internet relay is operated by Apple in locations around the world.

Different than a VPN
Unlike a traditional VPN, iCloud Private Relay's dual-hop architecture ensures no single party has access to both the user's IP address and the details of their browsing activity. Private Relay also does not allow users to represent themselves as connecting from a different country or region.

As the user browses, their original IP address is visible to the first internet relay and to the network they are connected to (e.g., their home ISP or cellular service). However, the website names requested by the user are encrypted and cannot be seen by either party.

The second internet relay (also known as the "egress proxy") has the role of assigning the Relay IP address they'll use for the session, decrypting the website name the user has requested and completing the connection. The second internet relay has no knowledge of the user's original IP address and receives only enough location information to assign them a Relay IP address that maps to the region they are connecting from, conforming to the IP Address Location preference they selected in Private Relay settings. The second internet relay is operated by third-party partners who are some of the largest content delivery networks (CDNs) in the world.

The system is designed to allow new partners to be onboarded in order to deliver greater diversity of providers, more global coverage, and enhanced routing while maintaining the same innovative dual-hop design.

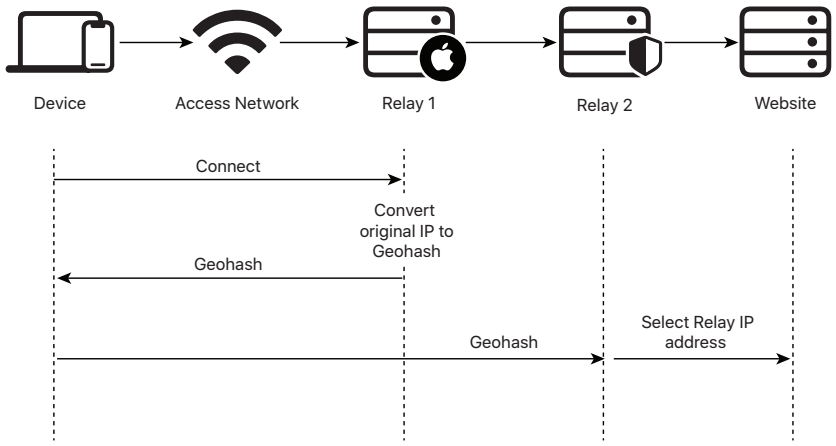
IP Addresses, Identity, and Location

Private Relay is designed to protect users' privacy, while maintaining sufficiently accurate location information to support a personalized experience on the web. It does not provide any methods to spoof location or circumvent regional content restrictions. The Relay IP addresses issued by Private Relay are representative IP addresses that map to the actual country or region the user is connecting from.

The selection of Relay IP addresses is influenced by the user's original IP address and IP Address Location setting preference. Furthermore, since the second internet relay does not know the original IP address of the user, the Relay IP addresses rotate over time and between sessions, helping to prevent their use as a stable identifier for the user.

Geohash
A geohash is a unique multi-character representation of a specific geographic location on earth. It subdivides the globe into a series of grid-like boxes, which get more precise based on the number of letters and digits.

The first internet relay uses a traditional geo-IP lookup to determine which geographic area best represents the user's original IP address. It then sends this information back to the user's device in the form of a geohash (truncated to four characters, representing roughly an 800 km^2 area).



If the user has selected "Maintain general location," the user's device will share the geohash information with the second internet relay. This information allows the second internet relay to select a representative Relay IP address from a pool of addresses assigned to the location.

If "Use country and time zone" is selected, geohash information is not shared and the second internet relay will select a Relay IP address from the much larger region that represents the country and time zone the user is connecting from.

Exclusive IP addresses
The Relay IP addresses used by Private Relay are not used or shared for any purpose other than to provide the Private Relay service. The entire list is published to the major geo-IP industry databases and is posted publicly by Apple at: mask-api.icloud.com/egress-ip-ranges.csv

The second internet relay has no knowledge of the user's original IP address. This helps ensure the selection of a Relay IP address is random within the corresponding geohash or country information, and helps prevent any manipulation or spoofing of location.

Websites and apps can continue to use existing location mechanisms, such as geo-IP mappings, to map the location provided by the Relay IP address. If required, Core Location APIs are available to request a precise location from the user with explicit permission.

Transport and Security Protocols

Private Relay uses cutting-edge transport and security protocols to make sure that the routing path is highly efficient without needing to compromise on security or privacy. These include protocols to proxy internet connections, protect DNS name lookups, and authenticate users when connecting to Private Relay in order to prevent fraud.

Connection proxying

Connections from Safari and apps that are protected by Private Relay use the two most common internet transport protocols—TCP and UDP. To proxy these connections, Private Relay uses technology being developed by the MASQUE working group at the Internet Engineering Task Force (IETF). Specifically, MASQUE is a way of using HTTP/3 and QUIC as secure proxying technologies.

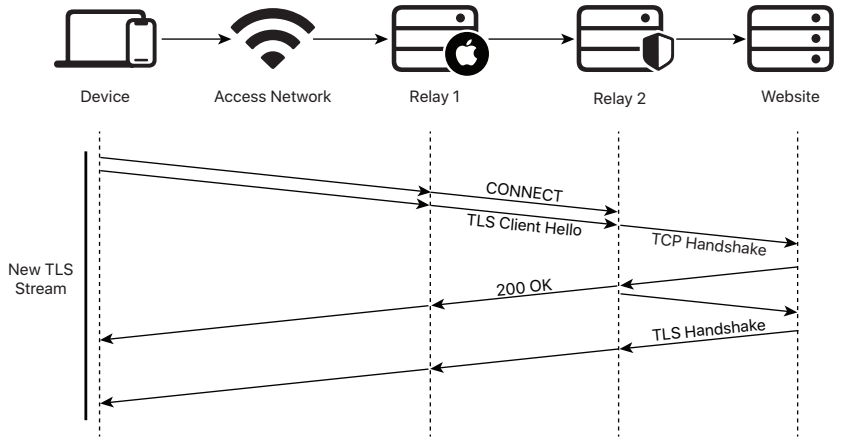
QUIC transport protocol

QUIC (RFC 9000) is a general-purpose transport layer network, standardized by the IETF in May 2021. Connections using QUIC can achieve great performance even in poor network environments by taking advantage of improved loss recovery. QUIC also allows connections to easily switch between network interfaces, allowing connectivity to be maintained as users move between Wi-Fi and cellular networks.

Private Relay takes particular advantage of some features of QUIC to make proxying connections more efficient and secure. QUIC allows multiplexing different streams of data, so all of the connections to websites can be sent over a single QUIC connection. QUIC also supports proxying unreliable datagrams, making it better for accessing servers that run UDP.

QUIC has TLS 1.3 built in, providing a strong cryptographic handshake to establish an encrypted session between devices and the proxies. To authenticate the proxies, devices validate the raw public key sent in the TLS handshake, and compare it to an expected value shared in an authenticated configuration separately. QUIC uses the result of the handshake to protect subsequent traffic during this session.

Private Relay uses both the CONNECT and CONNECT-UDP methods in HTTP/3 to set up connections quickly. For connections to websites that support TLS or QUIC, the initial TLS handshake messages are sent in the same set of data as the proxy request, removing the need to wait for replies from the proxies.



In networks where QUIC traffic is blocked, devices use the CONNECT method of HTTP/2 to communicate with the proxies, with the same requirement for TLS 1.3 and raw public keys.

DNS name resolution

DNS is the system that translates server names into IP addresses when using the internet. The ability to observe DNS lookups allows potential trackers to monitor user activity. To protect the privacy of DNS name resolution for all queries sent by the device and prevent such tracking, Private Relay uses Oblivious DNS over HTTPS (ODoH).

Oblivious DNS over HTTPS (ODoH)
ODoH adds a layer of public key encryption, as well as a network proxy between devices and DNS servers. The combination of these two added elements is designed such that only the user has access to both the DNS messages and their original IP address at the same time.

ODoH sends DNS queries through the first internet relay, so the DNS server cannot identify the user issuing a query. Each query itself is padded and encrypted using Hybrid Public Key Encryption (HPKE) to help ensure that the first internet relay cannot tell the domain name a user is looking up.

To ensure that DNS answers retrieved over ODoH are correct for the network that the device is on, the device is able to learn its public IP address subnet from the first internet relay and send that value in the encrypted query to the DNS server using the EDNS0 Client Subnet option.

Safari and unencrypted HTTP, which use connection proxying, do not need to first do ODoH queries. They connect through the proxy using names instead of IP addresses.

Relay access and fraud prevention

Private Relay is designed to ensure only valid Apple devices and accounts in good standing are allowed to use the service. Websites that use IP addresses to enforce fraud prevention and anti-abuse measures can trust that connections through Private Relay have been validated at the account and device level by Apple.

Built-in fraud prevention
An important part of Private Relay is enforcing several anti-abuse and anti-fraud techniques as users connect. Additionally, the Relay IP address assigned to users will remain stable during a browsing session, making sure websites see a consistent address. The combination of stable Relay IP addresses and fraud prevention is intended to provide websites with added trust when seeing connections from Private Relay users.

For a device to connect to iCloud Private Relay, it must first be authorized. Authorization is performed by presenting a valid, anonymous token based on RSA blind signatures. These signatures are sent as one-time-use tokens to each proxy when establishing a connection, separating legitimate from illegitimate devices. The proxies can validate the tokens with a public key to validate that the user is legitimate, without actually identifying the user. Tokens and keys are rotated daily to ensure users have authenticated recently. The proxies also perform asynchronous double-spend prevention to stop a token from being shared and used for fraudulent access.

To generate this blind signature, the user's device connects to an Apple server and is authenticated. To ensure only Apple devices and valid iCloud+ accounts can use Private Relay, the server performs device and account attestation using the Basic Attestation Authority (BAA) server prior to vending out tokens. To mitigate abuse, rate limiting restricts how many tokens a user's device can retrieve per day.

Logging
Private Relay's design, combined with a minimal logging policy, ensures that proxy logs do not contain enough information to connect a user's IP address or account information with their browsing activity.

The information logged by Private Relay contains no unique identifiers and is limited to the following, for the sole purpose of operating and improving the service:

- Connection properties and performance metrics
- Network and region information derived from IP address
- Anonymous token validation success rate and performance
- Private Relay system resource usage

The following fields related to anonymous token issuance are logged as a part of Private Relay's fraud prevention and anti-abuse measures, but cannot be correlated with connection information:

- iCloud account, software version, and request timestamp

Coverage and Compatibility

Private Relay is designed to be always-on and completely transparent, protecting the user without any noticeable impact to their day-to-day experience. However, there are some cases where Private Relay may not be applicable, or the service may be unavailable, as detailed below. In these instances, Private Relay is designed to provide clear status information and control to the user, and provide appropriate controls to enterprises and network operators that might require the ability to audit all traffic on their network.

Local and corporate network servers
Private Relay only protects connections on public internet servers, while still allowing users to access local or private servers directly with Private Relay enabled. This is great for accessing servers on a corporate network or interacting with devices on the local network.

If a proxy or ODoH server detects that a specific server name is not a public internet name, it instructs the device to try to access the server directly over the local network. For added protection, the device will never allow direct connections to names that are on the DuckDuckGo known tracker list.

Private Relay will not attempt to proxy traffic that the device knows is specific to the local network, such as an IP address on the local subnet.

Cellular services
Cellular services, such as Multimedia Messaging Service (MMS), telephony services (XCAP), Entitlement Server access, tethering traffic, and Visual Voicemail, do not use Private Relay. These services are always accessed directly.

Enterprises and device management

Most managed networking settings that are used by enterprises take precedence over Private Relay. If a device has a VPN installed, for either enterprise or personal reasons, traffic that goes through the VPN will not use Private Relay. Similarly, a proxy configuration, such as a Global Proxy, will be used instead of Private Relay.

If a device is supervised by an organization, a management profile can be used to disable Private Relay on the device.

Custom DNS settings

If a user has configured custom-encrypted DNS settings using a profile or an app, the DNS server specified will be used instead of ODoH. Safari connections and all unencrypted HTTP connections will also resolve names using the specified DNS server prior to routing through Private Relay.

An unencrypted DNS server provided by a local network or manually edited in Settings (iOS) or System Preferences (macOS) will not be used for iCloud Private Relay traffic.

Network settings

Some organizations might be required to audit all network traffic by policy. To comply with such a requirement, these networks can block access to Private Relay. Users will be alerted that they need to either disable Private Relay for the network or choose another network.

The fastest and most reliable way to do this is to return a negative answer from the network's DNS resolver, preventing DNS resolution for the **mask.icloud.com** and **mask-h2.icloud.com** hostnames necessary for Private Relay traffic.

Conclusion

iCloud Private Relay introduces a new type of internet privacy service built right into the networking framework on Apple devices. It's built on the latest standard protocols, ensuring that enhanced privacy is coupled with a high-performance browsing experience. By taking this new approach to internet privacy, and including it with every iCloud+ subscription, Apple is providing device owners an easy way to meaningfully improve their privacy when browsing the internet, without compromising on user experience. The innovative multi-hop architecture that Private Relay is built on ensures that no single party—including Apple—can view both the IP address of the user and their browsing activity, a significant advancement in user privacy. The service is designed with existing internet frameworks in mind, allowing websites and servers to leverage existing geo-IP mapping mechanisms and building anti-abuse and fraud prevention mechanisms right into the system itself. Apple's privacy product principles are deeply integrated into Private Relay. To learn more about Apple's commitment to privacy, go to apple.com/privacy.